FUJITSU

shaping tomorrow with you

Deep Discovery™ Inspector on PRIMERGY provided by FUJITSU

標的型サイバー攻撃対策ソリューションで富士通をおすすめする理由

2018年10月

富士通株式会社

標的型サイバー攻撃対策セキュリティ

セキュリティは経営の課題

今日の世界ではサイバー空間とリアル空間が密接に連携しています。
その結果、サイバー空間でのセキュリティインシデントが、リアル空間にも非常に大きなインパクトやダメージを与えることになります。
サイバー攻撃の手口は日々巧妙化しており、全ての攻撃を完全に防ぐことは困難です。
これからは、サイバー攻撃を前提に、リスクが顕在化した状態から解決までの一連の処理（インシデントハンドリング）を考慮した対策が重要になります。
富士通はサイバー攻撃対策として、必要不可欠な次の運用プロセスでお客様をお守りします。

- リスク軽減
  攻撃状況や脆弱性情報等を継続的に監視することで、インシデントを早期に発見し、リスクを軽減。
- 被害の極小化
  インシデントが発生した場合に、迅速かつ適切な対応を行うことで被害を極小化。
- セキュリティ耐性強化
  定期的なアセスメントにより改善点を明確にし、改善していくことにより、サイバー攻撃への耐性を強化。

「富士通グループ 情報セキュリティへの取り組み」より一部抜粋
詳しくはこちらをご参照ください
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/index.html

標的型サイバー攻撃対策

「標的型サイバー攻撃」とは、特定の組織で保有する重要情報の窃取を目的に、その標的に特化して行われる一連の攻撃です。
標的型サイバー攻撃の攻撃手口は日々巧妙化しており、「気づけない攻撃」と言われています。
実に4社に1社の割合で侵入されているのが現状です。(注)
このような標的型サイバー攻撃対策には、ネットワーク通信を常に監視することが有効です。
攻撃を隠蔽されやすいサーバやクライアントに比べ、 ネットワーク通信は攻撃者の活動痕跡隠蔽が難しく、常に監視することで、侵入した脅威の早期検出を可能にします。

ネットワーク監視対象組織における脅威検出割合 (2017年) 出典:トレンドマイクロ社 「国内標的型サイバー攻撃分析レポート2018年版」

(注) トレンドマイクロ社 「国内標的型サイバー攻撃分析レポート2018年版」より

Deep Discovery™ Inspector on PRIMERGY provided by FUJITSU

Deep Discovery™ Inspector on PRIMERGYは、気付くことが難しい標的型攻撃や巧妙化するランサムウェアを、ネットワーク全体に渡って検知・可視化することができるネットワーク監視ソリューションです。
従来のセキュリティ対策ではカバーしきれていない、攻撃者によるシステム内部の探索と攻撃を複数の脅威検出エンジンにより可視化、所在のはっきりしない脅威を突き止めます。

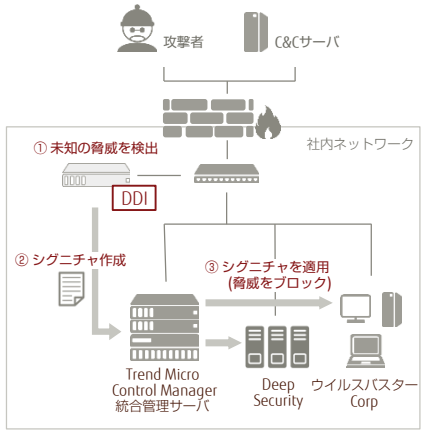
Deep Discovery™ Inspector on PRIMERGY

事前準備	感染	端末制御	権限掌握	情報収集	漏洩
・攻撃目標の調査 ・C&Cサーバ準備 ・マルウェア作成	・標的形メール ・不正Web閲覧 ・脆弱性を付く攻撃	・C&C通信 ・バックドア設定 ・攻撃ツールDL	・社内サーバ探索 ・感染拡大 ・管理者権限剥奪	・機密情報の収集	・機密情報を圧縮送信

検出した未知の脅威を迅速に駆除（Connected Threat Defense機能）

検出した未知の脅威に対応するシグネチャを生成、トレンドマイクロ社の各製品へ自動配信します。
即座に未知マルウェアの駆除や不審URLへの通信遮断を行うことで、お客様ITシステムをセキュリティ脅威から保護します。

巧妙化を続け増大する脅威への対策は、この様な多段的な防御が効果的と言えますが、運用雑化の懸念があることも事実です。
富士通ではお客様の運用負担を軽減するサービスを提供、セキュリティ対策による安心感に、さらに運用の安心感をプラスします。



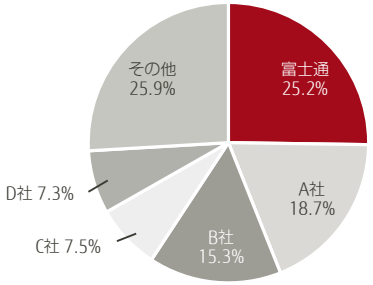
国内トップレベルの導入実績と製品ラインナップの安心感

国内トップレベルの導入実績

トレンドマイクロ社各製品の導入実績は国内トップレベルで、その中でもサーバ&クラウドセキュリティソリューションであるTrend Micro Deep Securityについては、3年連続売上No.1の実績があります。
Deep Discovery Inspector on PRIMERGY provided by FUJITSUは、 Trend Micro Deep Securityと連携、発見した未知マルウェアの定義ファイルをすぐに適用し、お客様ビジネスがセキュリティリスクにさらされる時間を最小化します。

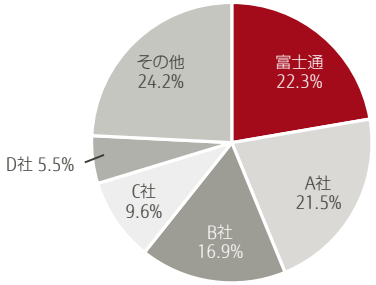
また、採用されているFUJITSU Server PRIMERGYは2017年の国内サーバ市場（出荷額）では3年連続、x86サーバ市場（出荷額）では2年連続国内シェア第1位を獲得しました。
システムとハードウェア両面におけるこれらの実績への信頼感も、富士通のお客様に選ばれる理由となっています。

国内サーバ市場
ベンダー別シェア (出荷額) (2017年)



出典 IDC Japan, Japan Quarterly Server Tracker CY18Q1 (Share by Company)
承諾番号: IDCJ-18-0735

国内x86サーバ市場
ベンダー別シェア (出荷額) (2017年)



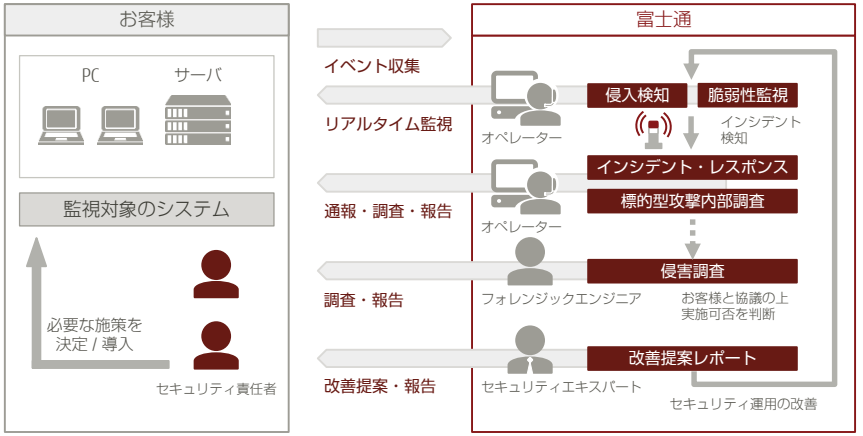
出典 IDC Japan, Japan Quarterly Server Tracker CY18Q1 (Share by Company) Japan Product category : x86 Server
承諾番号: IDCJ-18-0735

製品から教育や運用サービスまでの豊富なラインナップ

様々なセキュリティソリューションからサーバなどのハードウェア各製品まで、一貫して取り揃えています。
また、導入や後述しますセキュリティ運用サービスのほか、各セキュリティ教育などの幅広いラインナップは、お客様に安心してお使いいただける理由の一つになっています。

FUJITSU Security Solution グローバルマネージドセキュリティサービス

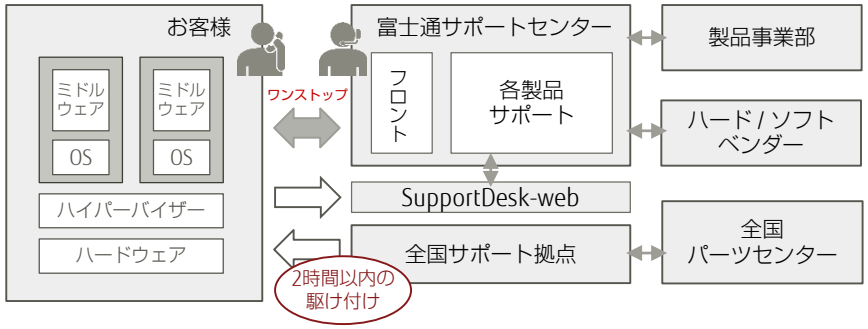
お客様自身では対応が難しい、24時間365日のリアルタイム監視、的確なインシデント対応といった継続的なセキュリティ運用強化支援など、サイバー攻撃に対応するためのセキュリティ運用サービスを提供します。
重大インシデント発生時には、高い技能を有するエキスパートが、課題解決に向けてサポートいたします。
企業・組織を標的としたサイバー攻撃の増加で、深刻さが増している現在のビジネス環境において、お客様ビジネス継続性へのリスクを最小化します。



安心サポート

ワンストップサポート

複数のソフトウェア・ハードウェアのサポート窓口を一本化したワンストップサポートを提供、お客様の運用負担を軽減します。



クイックレスポンス

サーバやストレージなど、障害受付から2時間以内を目標にサービスエンジニアが訪問し、迅速に修理、ビジネスへの影響を最小限に止めます。

- 製品障害対応の認定者を全国約850拠点、約8,000名配置
- パーツセンターを東西補給拠点を核に全国約100か所に配備

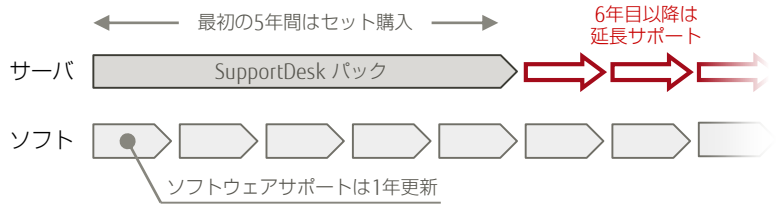
プロアクティブ

装置自らサポート窓口に連絡するリモート通報でのハードウェア障害・予兆アラーム通知や、ハードウェアの定期点検によりハードウェアトラブルの未然防止を図ります。

長いサポート期間

サポートはソフトウェアサポートとサーバサポートの組み合わせでサポートします。
基本サポート契約は1年毎更新ですが、サーバサポートでは、サーバのサポート期限である5年間分をセットにしたお得なFUJITSU Managed Infrastructure Service SupportDesk パックもご用意しています。
6年目以降のサーバサポートについては、ベストエフォート型の延長サポートも提供していますので、富士通のDeep Discovery Inspector on PRIMERGYはお客様環境に合わせて長期間お使いいただけます。

例 SupportDeskパックとソフトウェアサポートの組み合わせ

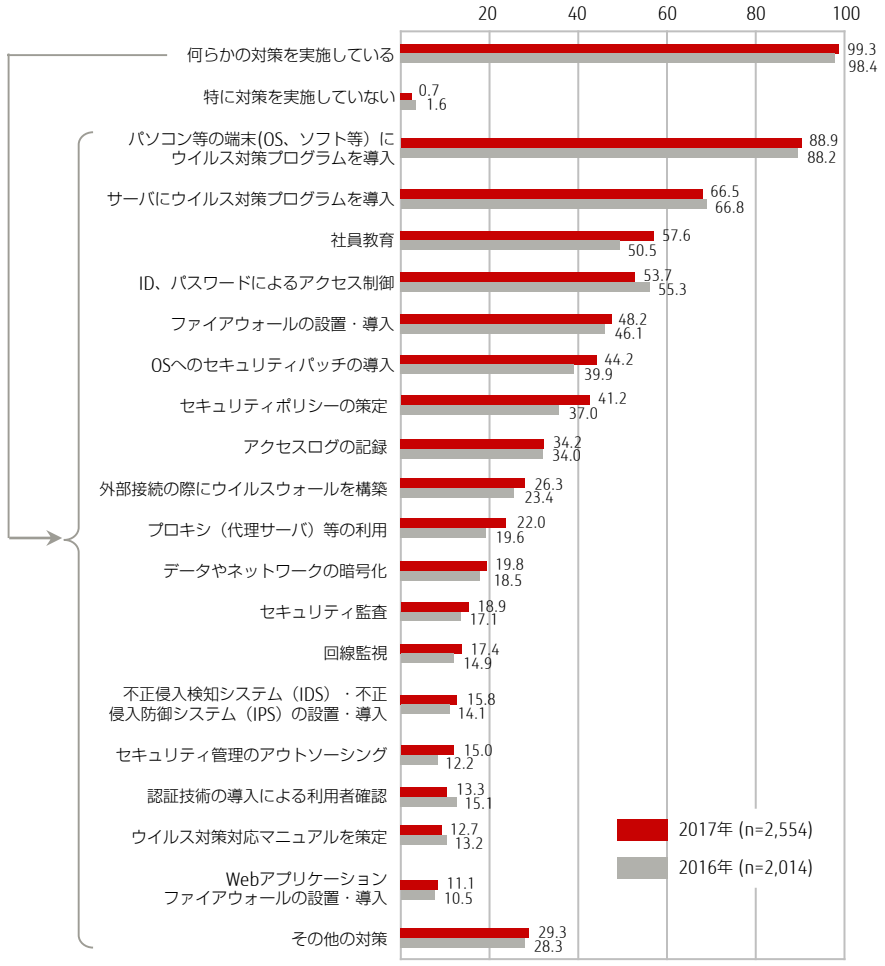


(注)将来リリースされるDeep Discovery Inspectorのハードウェア要件を充たしている場合に限ります。

※ 記載のサービス時間やサービス内容はご契約により異なります。

参考データ

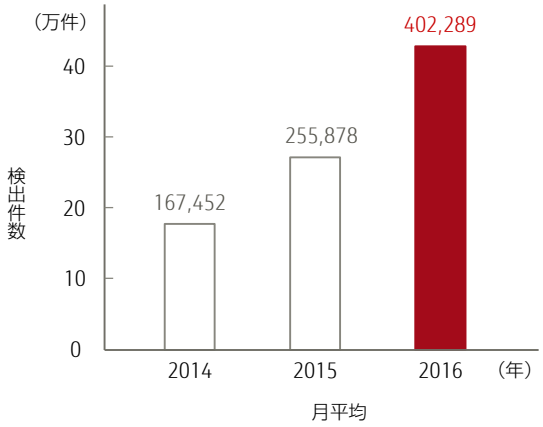
企業における情報セキュリティ対策の実施状況（複数回答）



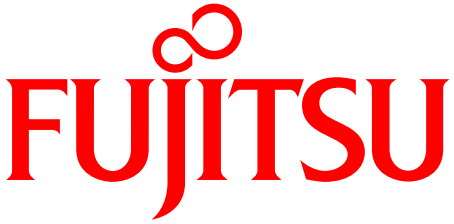
（注）情報通信ネットワーク（企業内・企業間通信網やインターネット）利用企業に占める割合

総務省「通信利用動向調査」 http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

標的型サイバー攻撃による内部活動月平均検出件数



トレンドマイクロ社：
国内標的型サイバー攻撃分析レポート2017年版 ～ 巧妙化と高度化を続ける「気づけない」攻撃 ～



shaping tomorrow with you

お問い合わせ先

富士通コンタクトライン
0120-933-200
受付時間 9:00～17:30
（土曜・日曜・祝日・当社指定の休業日を除く）

富士通株式会社
〒105-7123 東京都港区東新橋1-5-2 汐留シティセンター